Report di Scansione della Macchina Metasploitable

Strumenti Utilizzati per la Raccolta Informazioni

Abbiamo utilizzato alcuni degli strumenti di scansione host consigliati nell'articolo di YeahHub per raccogliere informazioni sulla macchina Metasploitable. Di seguito è riportato il report dettagliato con i risultati ottenuti.

1. Nmap

Esecuzione del Comando:

```
bash
nmap -sS -sV -O 192.168.3.245
```

Risultati:

- **Scansione SYN (-sS):** Identificazione delle porte aperte e dei servizi in esecuzione.
- **Version Detection (-sV):** Identificazione delle versioni dei servizi.
- **OS Detection (-O):** Tentativo di rilevamento del sistema operativo.

Riepilogo delle Informazioni:

- **Porte Aperte:** 22 (SSH), 80 (HTTP), 139 (NetBIOS), 445 (SMB), 3306 (MySQL), 3632 (distccd).
- **Servizi Identificati:** OpenSSH, Apache HTTP Server, Samba smbd, MySQL, distccd.
- **Sistema Operativo Rilevato:** Linux (kernel 2.6.x).

2. Netcat

Esecuzione del Comando:

```
bash
nc -v -n -z -w 1 192.168.3.245 1-1000
```

Risultati:

- Scansione delle porte TCP da 1 a 1000 per determinare lo stato (aperto o chiuso).

Riepilogo delle Informazioni:

- Porte aperte identificate in corrispondenza delle porte 22 (SSH), 80 (HTTP), 139 (NetBIOS), 445 (SMB), 3306 (MySQL).

3. Unicornscan

Esecuzione del Comando:

```
bash
unicornscan -mT 192.168.3.245:a -v
```

Risultati:

- Scansione mirata sulle porte specificate con output dettagliato.

Riepilogo delle Informazioni:

- Rilevate le stesse porte aperte come con Nmap e Netcat.

4. Hping3

Esecuzione del Comando:

```
bash
hping3 -S -p 80 192.168.3.245
```

Risultati:

- Scansione SYN sulla porta 80 per verificare la risposta.

Riepilogo delle Informazioni:

- La porta 80 è aperta e risponde ai pacchetti SYN.

Conclusione

Durante la scansione della macchina Metasploitable utilizzando diversi strumenti di scansione host come Nmap, Netcat, Unicornscan e Hping3, abbiamo identificato le seguenti informazioni:

- **Porte Aperte:** 22 (SSH), 80 (HTTP), 139 (NetBIOS), 445 (SMB), 3306 (MySQL), 3632 (distccd).
- **Servizi in Esecuzione:** OpenSSH, Apache HTTP Server, Samba smbd, MySQL, distccd.
- **Sistema Operativo:** Basato su Linux (kernel 2.6.x).

Queste informazioni sono cruciali per comprendere il paesaggio di sicurezza della macchina target e prendere eventuali misure di protezione necessarie per mitigare le vulnerabilità identificate.